

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

LONGHORN HD LLC.,

Plaintiff,

v.

NETSCOUT SYSTEMS, INC.,

Defendant.

§
§
§
§
§
§
§
§
§
§
§

Case No.

JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Longhorn HD LLC. (“LHD” or “Plaintiff”) for its Complaint against Defendant NetScout Systems, Inc. (“NetScout” or “Defendant”) alleges as follows:

THE PARTIES

1. LHD is a limited liability company organized and existing under the laws of the State of Texas, with its principal place of business located at 203 East Travis Street, Marshall, Texas 75670.

2. Upon information and belief, Defendant NetScout Systems, Inc. is corporation organized under the laws of the state of Delaware with a regular and established place of business in this judicial district at 915 Guardians Way, Allen, TX 75013. Upon information and belief, NetScout does business in Texas and in the Eastern District of Texas, directly or through intermediaries.

JURISDICTION

3. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1, *et seq.* This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

4. This Court has personal jurisdiction over Defendant. Defendant regularly conducts business and has committed acts of patent infringement and/or has induced acts of patent infringement by others in this Judicial District and/or has contributed to patent infringement by others in this Judicial District, the State of Texas, and elsewhere in the United States.

5. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391 because, among other things, Defendant is a defendant not resident in the United States, and thus may be sued in any judicial district pursuant to 28 U.S.C. § 1391(c)(3).

6. Defendant is subject to this Court's jurisdiction pursuant to due process and/or the Texas Long Arm Statute due at least to its substantial business in this State and Judicial District, including (a) at least part of its past infringing activities, (b) regularly doing or soliciting business in Texas, and/or (c) engaging in persistent conduct and/or deriving substantial revenue from goods and services provided to customers in Texas.

PATENTS-IN-SUIT

7. On October 11, 2005, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 6,954,790 (the "'790 Patent") entitled "Network-Based Mobile Workgroup System." A true and correct copy of the '790 Patent is available at <http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=6954790>.

8. On August 21, 2007, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 7,260,846 (the "'846 Patent") entitled "Intrusion Detection System."

A true and correct copy of the '846 Patent is available at <http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=7260846>.

9. LHD is the sole and exclusive owner of all right, title, and interest in the '790 Patent and the '846 Patent, (collectively, the "Patents-in-Suit"), and holds the exclusive right to take all actions necessary to enforce its rights to the Patents-in-Suit, including the filing of this patent infringement lawsuit. LHD also has the right to recover all damages for past, present, and future infringement of the Patents-in-Suit and to seek injunctive relief as appropriate under the law.

FACTUAL ALLEGATIONS

10. The Patents-in-Suit generally cover systems and methods for computer and network security.

11. The '790 Patent generally relates to technology for mobile workgroups' VPN and firewall systems. The technology further implements these mappings as the basis for secure gateways. The technology described in the '790 Patent was developed by Jan Forsl w at Interactive People Unplugged AB. By way of example, this technology is implemented today in VPNs that allow for mobile participation, further implementing network firewalls and gateways that allow for the VPNs to share resources with mobile devices.

12. The '846 Patent generally relates to technology for intrusion detection systems. The technology described in the '846 Patent was developed by Christopher Day at Steelcloud, Inc. By way of example, this technology is implemented today in intrusion detection systems ("IDS") and intrusion prevention systems ("IPS") that utilize machine-learning techniques to detect and prevent intrusions.

13. NetScout has infringed and is continuing to infringe one or more of the Patents-in-Suit by making, using, selling, offering to sell, and/or importing, and by actively inducing others

to make, use, sell, offer to sell, and/or importing, products that include security gateways, routers, control system security appliance, clouds, and components and software that provide or utilize firewall, VPN, IPSec, DNS, IDS/IPS, mobile security, and threat protection, as well as network-based mobile workgroup systems. Such products include at least the Arbor Threat Analytics, Arbor Edge Defense, Adaptive Services Intelligence, ATLAS Intelligence Feed, nGenius Packet Flow System, Packet Flow eXtender, nGeniusONE, and nGeniusPULSE products and associated software which utilize functionality that infringes the Patents-in-Suit (“Accused Products”).

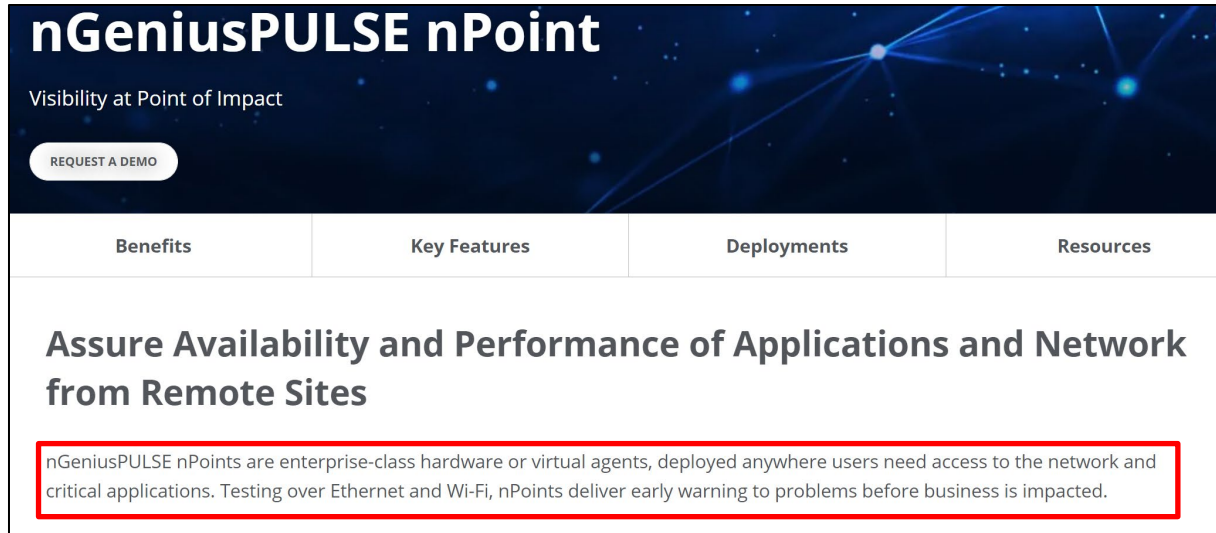
COUNT I
(Infringement of the ’790 Patent)

14. Paragraphs 1 through 13 are incorporated by reference as if fully set forth herein.

15. LHD has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the ’790 Patent.

16. Defendant has and continues to directly infringe the ’790 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’790 Patent. Such products include at least the nGeniusONE and nGeniusPULSE products and associated software.

17. For example, Defendant has and continues to directly infringe at least claim 1 of the ’790 Patent by making, using, offering to sell, selling, and/or importing into the United States products that include gateway devices that provide mobile user workgroups. The infringing systems include a network-based mobile workgroup system comprising a plurality of mobile client nodes, each mobile client node providing an interface for user interaction by a mobile user, for example, nGeniusONE and nGeniusPULSE products running on mobile devices, including but not limited to Android devices.



nGeniusPULSE nPoint
Visibility at Point of Impact

REQUEST A DEMO

Benefits Key Features Deployments Resources

Assure Availability and Performance of Applications and Network from Remote Sites

nGeniusPULSE nPoints are enterprise-class hardware or virtual agents, deployed anywhere users need access to the network and critical applications. Testing over Ethernet and Wi-Fi, nPoints deliver early warning to problems before business is impacted.

1

18. The Accused Products include a plurality of mobile service router nodes, each mobile service router node providing a mobile Virtual Private Network (VPN), or the functional equivalent thereof, to the mobile client nodes spanning multiple router hops and sites. Upon information and belief, the Accused Products further include a network address identifier (NAI) with which a user of a mobile client is uniquely identified to the mobile VPN system, for example, a device Media Access Control (“MAC”) address.

19. Additionally, the Accused Products include a set of firewall filters and route policies with which the workgroup is protected. Additionally, the mobile VPN provides each mobile client secure data access to the VPN and provides secure data access to each mobile client from within the mobile VPN, wherein a point of attachment of any mobile client node to the mobile VPN may change without affecting that mobile client node’s participation in the mobile VPN.

20. Defendant has and continues to indirectly infringe one or more claims of the ’790 Patent by knowingly and intentionally inducing others, including NetScout customers and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using,

¹ <https://www.netscout.com/product/npoint>.

offering to sell, selling and/or importing into the United States products that include infringing technology, such as NetScout client for mobile devices.

21. Defendant, with knowledge that these products, or the use thereof, infringe the '790 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '790 Patent by providing these products to end users for use in an infringing manner.

22. Defendant induced infringement by others, including end users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end users, infringe the '790 Patent, but while remaining willfully blind to the infringement.

23. LHD has suffered damages as a result of Defendant's direct and indirect infringement of the '790 Patent in an amount to be proved at trial.

24. LHD has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '790 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

COUNT II
(Infringement of the '846 Patent)

25. Paragraphs 1 through 13 are incorporated by reference as if fully set forth herein.

26. LHD has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the '846 Patent.

27. Defendant has and continues to directly infringe the '846 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '846 Patent. Such products include intrusion

detection systems and intrusion prevention systems including the NetScout Arbor Threat Analytics, Arbor Edge Defense, Adaptive Services Intelligence, ATLAS Intelligence Feed, nGenius Packet Flow System, Packet Flow eXtender.

28. For example, Defendant has and continues to directly infringe at least claim 7 of the '846 Patent by making, using, offering to sell, selling, and/or importing into the United States products that include systems that practice the claimed method alone, or in combination with other NetScout products or services.

29. The Accused Products are systems that perform an intrusion detection method comprising the steps of monitoring network traffic passing across a network communications path. For example, the nGenius Packet Flow System monitors network traffic. Additionally, upon information and belief, the nGenius Packet Flow System performs network traffic parsing:

Software-driven and Cost-effective Performance

The nGenius Packet Flow Switch (PFS) 5000 series models operate at speeds 1Gbps to 100Gbps, providing core packet broker functionality, such as filtering, load balancing, aggregation, and replication, wherever packet broker ports are needed. Specifically, the nGenius PFS 5000 series operates stand alone, like any other PFS switch in the portfolio, in remote sites where the small 1 Rackmount Unit (RU) form factor is ideal. Enabled with self-organizing mesh technology, the nGenius PFS 5000 series easily scales for large-scale network monitoring needs.



Scalability on Demand

The nGenius PFS 5000 series can be used in stand-alone deployments, or in combination with other Packet Flow System products, such as nGenius PFS 6000 blade-and-chassis model, which provides the industry's highest non-blocking throughput at 6Tbps. The NETSCOUT patented self-organizing mesh technology, pfsMesh™, enables dynamic scaling and self-healing connections between the packet flow systems – in the datacenter or across large distances.

High-port Count for Dense 10/40/100GbE Deployments

Packing a lot of interfaces into a compact form factor, the nGenius PFS 5000 series supports core network packet broker features, which includes filtering, load balancing, replication, and aggregation. Connect HD Fiber TAPs and any number of tools, including the NETSCOUT InfiniStream® platform, to the nGenius PFS 5000, and easily manage a diverse and complex monitoring network.

2

30. Additionally, upon information and belief, the Accused Products store individual components of said network packets in a database and construct multi-dimensional vectors from at least two of said stored individual components and applying at least one multi-variate analysis to said constructed multi-dimensional vectors, said at least one multi-variate analysis producing a corresponding output set. Additionally, the Accused Products establish a correlation between individual output sets based upon a selected metric to identify anomalous behavior.

² <https://www.netscout.com/product/ngenius-5000-series-packet-flow-switch>.

Arbor Threat Analytics

In a recent Network Management Megatrends study exploring NetSecOps convergence, it was revealed the 91% of enterprises had evolved their IT organizations to have at least some formal collaboration between their network and security groups, with at least 40% of them fully converged and sharing tools and processes. It also identified that 35% of the respondents were enabling collaboration by integrating the toolsets of network and security teams, with 16% overall having deployed actual tools that both the network and security teams shared. That said, 84% of network and security teams reported they lacked a shared data store that was consistent, current, and relevant to the task of collaboration.

Visibility and Analytics to Address Security Risks and Investigations

NETSCOUT delivers visibility deep within data centers and enterprise networks with Arbor Threat Analytics (ATA).

With the ability to promptly and efficiently detect, investigate, validate, and respond to threats, ATA serves as an early warning system of damaging incidents, with a rich source of data analytics to reduce the time cyber criminals can lurk in your network, thus minimizing risk to your company's resources and reputation.

Harnessing the Power of Smart Data for Security

The NETSCOUT approach, based on patented Adaptive Service Intelligence (ASI) technology, enables ATA to provide early detection, high-fidelity packet analysis and investigation, and integration with third-party SIEMs to help organizations reduce the threat from security-related incidents. This highly scalable, deep packet inspection engine leverages continuous, real-time monitoring of wire traffic for packet data with NETSCOUT InfiniStreamNG (ISNG) software and hardware appliances and vSTREAM virtual appliances. With ASI, threats will be detected and linked to detailed security forensics analysis with packet- and session- level evidence to complete a security incident triage and investigation, with ATA providing the logical, intuitive, contextual drill-downs.

Arbor Edge Defense

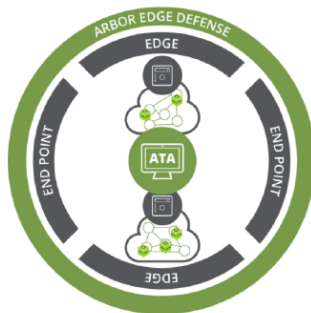


Figure 1: Arbor Threat Analytics provides visibility deep inside data centers, between the edge and endpoints, for any infrastructure, any application, and anywhere for threat detection, incident response, and forensic analysis, using the best data source for security and network ops. NETSCOUT's recently introduced Arbor Edge Defense is focused on security for beyond the perimeter.

³ <https://www.netscout.com/product/arbor-threat-analytics>.

31. The Accused Products classify the anomalous behavior as an event selected from the group consisting of a network fault, a change in network performance, and a network attack.

32. Defendant has and continues to indirectly infringe one or more claims of the '846 Patent by knowingly and intentionally inducing others, including NetScout customers and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States products that include infringing technology, such as IDS and IPS systems.

33. Defendant, with knowledge that these products, or the use thereof, infringe the '846 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '846 Patent by providing these products to end users for use in an infringing manner.

34. Defendant induced infringement by others, including end users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end users, infringe the '846 Patent, but while remaining willfully blind to the infringement.

35. LHD has suffered damages as a result of Defendant's direct and indirect infringement of the '846 Patent in an amount to be proved at trial.

36. LHD has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '846 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury for all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, LHD prays for relief against Defendant as follows:

- a. Entry of judgment declaring that Defendant has directly and/or indirectly infringed one or more claims of each of the Patents-in-Suit;
- b. An order pursuant to 35 U.S.C. § 283 permanently enjoining Defendant, its officers, agents, servants, employees, attorneys, and those persons in active concert or participation with it, from further acts of infringement of the Patents-in-Suit;
- c. An order awarding damages sufficient to compensate LHD for Defendant's infringement of the Patents-in-Suit, but in no event less than a reasonable royalty, together with interest and costs;
- d. Entry of judgment declaring that this case is exceptional and awarding LHD its costs and reasonable attorney fees under 35 U.S.C. § 285; and,
- e. Such other and further relief as the Court deems just and proper.

Dated: November 5, 2020

Respectfully submitted,

/s/ Vincent J. Rubino, III

Alfred R. Fabricant

NY Bar No. 2219392

Email: afabricant@fabricantllp.com

Peter Lambrianakos

NY Bar No. 2894392

Email: plambrianakos@fabricantllp.com

Vincent J. Rubino, III

NY Bar No. 4557435

Email: vrubino@fabricantllp.com

FABRICANT LLP

230 Park Avenue, 3rd Floor W.

New York, NY 10169

Telephone: (212) 257-5797

Facsimile: (212) 257-5796

John Andrew Rubino
NY Bar No. 5020797
Email: jarubino@rubinoip.com
RUBINO LAW LLC
830 Morris Turnpike
Short Hills, NJ, 07078
Telephone: (973) 535-0920
Facsimile (973) 535-0921

Justin Kurt Truelove
Texas Bar No. 24013653
Email: kurt@truelovelawfirm.com
TRUELOVE LAW FIRM, PLLC
100 West Houston
Marshall, Texas 75670
Telephone: (903) 938-8321
Facsimile: (903) 215-8510

**ATTORNEYS FOR PLAINTIFF
LONGHORN HD LLC.**